JOURNAL OF ALGEBRA **125**, 519–523 (1989)

Generalization of the Von Staudt–Clausen Theorem

I. DIBAG

Faculty of Engineering and Sciences, Bilkent University, P.O.B. 8, Maltepe, Ankara, Turkey

Communicated by Walter Feit

Received May 2, 1988

The localization $L_S(x)$ of $\log(1+x)$ at a set of primes S is defined by taking those powers of x in the logarithmic series for $\log(1+x)$ which lie in the span of S. The functional inverse $L_S^{-1}(x)$ of $L_S(x)$ also localizes the functional inverse e^x-1 of $\log(1+x)$ and a generalization of the Von Staudt–Clausen theorem is proved for the even coefficients in the power series expansion for $x/L_S^{-1}(x)$. This reduces to the Von Staudt–Clausen theorem when S is the set of all primes and to a weaker version of Theorem 3.9 of I. Dibag (*J. Algebra* **87** (1984), 332–341) when S consists of a single prime.

INTRODUCTION

The Bernoulli numbers B_n are defined by the power series expansion $x/e^x-1=1-\frac{1}{2}x+\sum_{n=1}^{\infty}(B_n/(2n)!)\,x^{2n}$. The Von Staudt–Clausen theorem asserts that $B_n=-\sum_{p-1/2n}(1/p) \pmod{Z}$. Let p be a prime and define $L_p(x)=\sum_{k=0}^{\infty}(x^{p^k}/p^k)=x+x^p/p+x^{p^2}/p^2+x^{p^3}/p^3+\cdots$ and $x/L_p^{-1}(x)=\sum_{n=0}^{\infty}(a_n/(n(p-1))!)\,x^{n(p-1)}$. Then [2, Theorem 3.9] states that $a_n=-(1/p) \pmod{Z}$. In this note we aim to establish a unified theorem which can accommodate both results. For this purpose we define the localization $L_S(x)$ of $\log(1+x)$ at a set of primes S by taking those powers of x in the logarithmic series for $\log(1+x)$ which lie in the span of S. The functional inverse $L_S^{-1}(x)$ of $L_S(x)$ also localizes the functional inverse e^x-1 of $\log(1+x)$. If $x/L_S^{-1}(x)=\sum_{n=0}^{\infty}b_n(x^n/n!)$ then the main result of this note, Theorem 1.4, states that

$$b_{2n}=-\sum_{\substack{p-1/2n\\ p\in S}}\frac{1}{p} \pmod{Z}.$$

This reduces to the Von Staudt–Clausen theorem itself when S is the set of all primes and to a slightly weaker version of [2, Theorem 3.9] when S consists of a single prime.

0021-8693/89 $3.00

1. Generalization of the Von Staudt–Clausen Theorem

Definition 1.1. For a set S of primes define the span $\mathbb{Q}_S$ of S by $\mathbb{Q}_S = (n \in Z / n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ for $p_i \in S$, $1 \leqslant i \leqslant k)$.

Definition 1.2. Define the localization $L_S(x)$ of $\log(1+x)$ by $L_S(x) = \sum_{n \in \mathbb{Q}_S} ((-1)^{n-1}/n)\, x^n$. Note that $L_S(x)$ is just $L_p(x)$ when S consists of p alone.

Definition 1.3. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = \sum_{j=0}^{\infty} b_j x^j$ be two power series. The star-product $f(x) * g(x)$ of $f(x)$ and $g(x)$ is defined by $f(x) * g(x) = \sum_{k=0}^{\infty} c_k x^k$, where $c_k = \sum_{ij=k} a_i b_j$.

Observation 1.4. $L_S(x) = *_{p \in S} L_p(x)$.

Let Z_p denote the subring of rationals which are p-integral.

Observation 1.5. If $f(x) \in Z_p[[x]]$ and $a \in Z_p$ then $f(x)^a \in Z_p[[x]]$.

Lemma 1.6. *If* $f(x) \in xZ_p[[x]]$ *then* $e^{L_p(x) * f(x)} \in Z_p[[x]]$.

Proof. Let $f(x) = \sum_{i=1}^{\infty} a_i x^i$, $a_i \in Z_p$.

$$
\begin{aligned}
e^{L_p(x) * f(x)} &= \exp\left(\sum_{k=1}^{\infty} x^k \left(\sum_{ip^j = k} \frac{a_i}{p^j} \right) \right) \\
&= \exp\left(\sum_{i=1}^{\infty} a_i \left(\sum_{j=0}^{\infty} \frac{(x^i)^{p^j}}{p^j} \right) \right) \\
&= \exp\left(\sum_{i=1}^{\infty} a_i L_p(x^i) \right) \\
&= \prod_{i=1}^{\infty} (e^{L_p(x^i) a_i} \in Z_p[[x]]
\end{aligned}
$$

since $e^{L_p(x^i)} \in Z_p[[x]]$ by [3, Proposition 1] and $(e^{L_p(x^i)})^{a_i} \in Z_p[[x]]$ by Observation 1.5 above.

Corollary 1.7. $e^{L_S(x)} \in Z_p[[x]]$ *for* $p \in S$.

Proof. Let $p \in S$ and take

$$
f(x) = \underset{\substack{p' \in S \\ p' \neq p}}{*} L_{p'}(x)
$$

in Lemma 1.6.

DEFINITION 1.8. Define integers $A_{q,k}$ by $(e^x-1)^k=\sum_{q\geqslant k} A_{q,k}(x^q/q!)$.

DEFINITION 1.9. Define integers $B_{q,k}$ by $(L_S^{-1}(x))^k=\sum_{q\geqslant k} B_{q,k}(x^q/q!)$.

DEFINITION 1.10. Define rational numbers b_n by $x/L_S^{-1}(x)=\sum_{n=0}^{\infty} b_n(x^n/n!)$.

LEMMA 1.11.

$$b_n=\sum_{\substack{k\leqslant n+1\\ k\in\mathbb{Q}_S}} \frac{(-1)^{k-1}}{k} B_{n,k-1}.$$

Proof.

$$\sum_{n=1}^{\infty} b_n\frac{x^n}{n!}=\frac{x}{L_S^{-1}(x)}=\frac{L_S(L_S^{-1}(x))}{L_S^{-1}(x)}$$

$$=\sum_{k\in\mathbb{Q}_S}\frac{(-1)^{k-1}}{k}(L_S^{-1}(x))^{k-1}$$

$$\sum_{k\in\mathbb{Q}_S}\frac{(-1)^{k-1}}{k}\left(\sum_{n\geqslant k-1} B_{n,k-1}\frac{x^n}{n!}\right)$$

$$=\sum_{n=1}^{\infty}\left(\sum_{\substack{k\leqslant n+1\\ k\in\mathbb{Q}_S}}\frac{(-1)^{k-1}}{k}B_{n,k-1}\right)\frac{x^n}{n!}.$$

Equating coefficients of x^n yields the lemma.

Let $E(x)=e^x-1$ and $L(x)=\log(1+x)$. $L\circ E(x)=E\circ L(x)=x$.

LEMMA 1.12. *Let $p\in S$. Then there exist $c_i\in Z_p$ such that, $B_{n,r}=\sum_{m_1+\cdots+m_s=r}(r!/m_1\ldots m_s!)\,e_2^{m_2}\cdots e_s^{m_s}A_{n,m_1+2m_2+\cdots+sm_s}$.*

Proof. Let $f=L_S^{-1}\circ L$ and expand $f(x)=\sum_{i=1}^{\infty} e_i x^i$, $e_1=1$. $f^{-1}(x)=(L_S^{-1}\circ L)^{-1}(x)=L^{-1}\circ L_S(x)=E\circ L_S(x)=e^{L_S(x)}-1\in Z_p[[x]]$ by Corollary 1.7. Then $f(x)\in Z_p[[x]]$ by [2, Corollary 2.7]. Hence $e_i\in Z_p$. $L_S^{-1}(x)=L_S^{-1}\circ L\circ E(x)=f(E(x))=f(e^x-1)=\sum_{i=1}^{\infty} e_i(e^x-1)^i$. We raise both sides to the rth-power, i.e.,

$$\sum_{n=1}^{\infty} B_{n,r}\frac{x^n}{n!}$$

$$=(L_S^{-1}(x))^r=\left(\sum_{i=1}^{\infty} e_i(e^x-1)^i\right)^r$$

$$= \sum_{m_1 + \cdots + m_s = r} \frac{r!}{m_1!...m_s!} e_2^{m_2} \cdots e_s^{m_s} (e^x - 1)^{m_1 + 2m_2 + \cdots + sm_s}$$

$$= \sum_{m_1 + \cdots + m_s = r} \frac{r!}{m_1!...m_s!} e_2^{m_2} \cdots e_s^{m_s} \left(\sum_n A_{n, m_1 + 2m_2 + \cdots + sm_s} \frac{x^n}{n!} \right)$$

$$= \sum_{n=1}^{\infty} \left(\sum_{m_1 + \cdots + m_s = r} \frac{r!}{m_1!...m_s!} e_2^{m_2} \cdots e_s^{m_s} A_{n, m_1 + 2m_2 + \cdots + sm_s} \right) \frac{x^n}{n!}.$$

Equating coefficients of x^n yields the lemma.

Observation 1.13. If $k \in Z$ is not a prime then k divides $(k-1)!$

THEOREM 1.14.

$$b_{2n} = - \sum_{\substack{p-1/2n \\ p \in S}} \frac{1}{p} \pmod{Z}.$$

Proof. (1) $b_{2n} = \sum_{k \leqslant 2n+1, k \in \mathbb{Q}_S} ((-1)^{k-1}/k)\, B_{2n, k-1}$ by Lemma 1.11.

(2) $$B_{2n, k-1} = \sum_{m_1 + \cdots + m_s = k-1} \frac{(k-1)!}{m_1!...m_s!} e_2^{m_2} ... e_s^{m_s} A_{2n, m_1 + 2m_2 + \cdots + sm_s}$$

by Lemma 1.12. Suppose $k \in \mathbb{Q}_S$ is not a prime. Then $k-1 = m_1 + m_2 + \cdots + m_s \leqslant m_1 + 2m_2 + \cdots + sm_s$ and thus $(k-1)!/(m_1 + 2m_2 + \cdots + sm_s)!$ $k/(k-1)!$ by Observation 1.13 and $(m_1 + 2m_2 + \cdots + sm_s)!/A_{2n, m_1 + 2m_2 + \cdots + sm_s}$ by [5, Sect. 1.5, Lemma 2]. Thus $A_{2n, m_1 + 2m_2 + \cdots + sm_s} = 0 \pmod{k}$, $e_2^{m_2} \cdots e_s^{m_s} \in Z_p$ $\forall p \in S$ and $k \in \mathbb{Q}_S$ and thus the denominator of $e_2^{m_2} \cdots e_s^{m_s}$ is prime to k. Hence $B_{2n, k-1} = 0 \pmod{k}$ and $((-1)^{k-1}/k)\, B_{2n, k-1} \in Z$. Suppose $k = p$ is a prime in S. Let $m_i \geqslant 1$ for some $i \geqslant 2$. Then $m_1 + 2m_2 + \cdots + sm_s \geqslant m_1 + m_2 + \cdots + m_s + (i-1)\, m_i \geqslant (p-1) + 1 = p$. Thus $p/p!/(m_1 + 2m_2 + \cdots + sm_s)!/A_{2n, m_1 + 2m_2 + \cdots + sm_s}$, $e_2^{m_2} \cdots e_s^{m_s} \in Z_p$ and hence $((p-1)!/m_1! \cdots m_s!)\, e_2^{m_2} \cdots e_s^{m_s} A_{2n, m_1 + 2m_2 + \cdots + sm_s} = 0 \pmod{k}$. Hence the only term in Eq. (2) that is possibly not zero mod p is the one corresponding to the sequence $m_1 = p-1$ and $m_j = 0$ for $j \geqslant 2$ and we thus deduce from Eq. (2) that $B_{2n, p-1} = A_{2n, p-1} \pmod{p}$. If $p-1$ does not divide $2n$ then $A_{2n, p-1} = 0 \pmod{p}$ by [5, Sect. 1.5, Lemma 2]. Hence $B_{2n, p-1} = 0 \pmod{p}$ and $((-1)^{p-1}/p)\, B_{2n, p-1} \in Z$. If p is an odd prime and $(p-1)$ divides $2n$ then $A_{2n, p-1} = -1 \pmod{p}$ by [5, Sect. 1.5, Lemma 2]. Hence $B_{2n, p-1} = -1 \pmod{p}$ and $((-1)^{p-1}/p)\, B_{2n, p-1} = -1/p \pmod{Z}$ in Eq. (1). If $p = 2$ then $A_{2n, p-1} = A_{2n, 1} = 1 = 1 \pmod{p}$ and $B_{2n, p-1} = 1 \pmod{p}$ and $((-1)^{p-1}/p)\, B_{2n, p-1} = -1/p \pmod{Z}$. We thus obtain from Eq. (1) that

$$b_{2n} = - \sum_{\substack{p-1/2n \\ p \in S}} \frac{1}{p} \pmod{Z}.$$

COROLLARY 1.15. *The Von Staudt–Clausen theorem.*

Proof. Take S to be the set of all primes.

COROLLARY 1.16. *Let* $x/L_p^{-1}(x) = \sum_{n=0}^{\infty} b_n(x^n/n!)$. *Then*

$$b_{2n} = \begin{cases} -1/p \pmod{Z} & \text{if } 2n = 0 \pmod{(p-1)} \\ 0 \pmod{Z} & \text{if } 2n \neq 0 \pmod{(p-1)}. \end{cases}$$

Proof. Take $S = (p)$.

Note that Corollary 1.16 is a somewhat weaker version of [2, Theorem 3.9] whih includes (i) and also states that $b_n = 0$ if $n \neq 0 \pmod{(p-1)}$.

REFERENCES

1. G. BACHMANN, "Introduction to p-adic Numbers and Valuation Theory," Academic Press, New York, 1964.
2. I. DIBAG, An analogue of the Von Staudt–Clausen theorem, *J. Algebra* **87** (1984), 332–341.
3. J. DIEUDONNÉ, On the Artin–Hasse exponential series, *Proc. Amer. Math. Soc.* **8** (1957), 210–214.
4. B. DWORK, On the zeta-function of a hypersurface, *Inst. Hautes Études Sci. Publ. Math.* **12** (1962), 7–17.
5. H. RADEMACHER, "Topics in Analytic Number Theory." Springer-Verlag, Berlin/ Heidelberg/New York, 1973.